WHAT IS CLAIMED IS:

1. A method for third party recovery of encryption certificates in a Public Key Infrastructure (PKI) comprising:

convincing a second enterprise official to designate an encryption certificate of a user as approved for recovery, the convincing performed by a first enterprise official, the first enterprise official desiring to recover the encryption certificate, the second enterprise official having authorization to designate the encryption certificate as approved for recovery;

designating the encryption certificate as approved for recovery;

convincing a third enterprise official to execute recovery of the encryption certificate, the convincing performed by the first enterprise official, the third enterprise official having authorization to execute recovery of the encryption certificate;

recovering the encryption certificate by the third enterprise official; and

providing the encryption certificate to the first enterprise official by the third enterprise official, wherein the first enterprise official, the second enterprise official, and the third enterprise official are members of an enterprise.

2. The method according to claim 1, wherein the user is a current member of the enterprise.

3. The method according to claim 2, wherein the second enterprise official comprises a personal recovery approval associated with the user, the association listed in a directory of the enterprise.

4. The method according to claim 3, further comprising accessing the directory by the first enterprise official to determine the personal recovery approval associated with the user, the accessing occurring before the convincing the second enterprise official to designate the encryption certificate of the user as approved for recovery.

5. The method according to claim 4, wherein the designating the encryption certificate as approved for recovery comprises:

accessing a registration web server by the personal recovery approval;

sending a signature certificate of the personal recovery approval to the registration web server by the personal recovery approval to authenticate the personal recovery approval to the registration web server;

requesting, by the personal recovery approval, that the encryption certificate be designated as recoverable;

querying the directory by the registration web server to verify that the personal recovery approval is allowed to approve recovery of the encryption certificate of the user; and

signaling a key recovery authority by the registration web server to tag the encryption certificate of the user as recoverable.

6. The method according to claim 4, wherein the recovering the encryption certificate by the third enterprise official comprises:

accessing a registration web server by the third enterprise official;

sending a signature certificate of the third enterprise official to the registration web server by the third enterprise official to authenticate the third enterprise official to the registration web server;

requesting, by the third enterprise official, that the encryption certificate be recovered;

querying the directory by the registration web server to verify that the third enterprise official is allowed to recover the encryption certificate of the user; and

signaling a key recovery authority by the registration web server to send the encryption certificate of the user to the third enterprise official.

7. The method according to claim 1, wherein the user is a former member of the enterprise.

8. The method according to claim 7, further comprising accessing a directory of the enterprise by the first enterprise official to determine a personal recovery approval associated with the user in the directory, the accessing occurring before the convincing the second enterprise official to designate the encryption certificate of the user as approved for recovery.

9. The method according to claim 8, further comprising notifying the first enterprise official by the directory that the user is not a member of the enterprise and has no associated personal recovery approval.

10. The method according to claim 7, wherein the designating the encryption certificate as approved for recovery comprises:

accessing a registration web server by the second enterprise official;

sending a signature certificate of the second enterprise official to the registration web server by the second enterprise official to authenticate the second enterprise official to the registration web server;

requesting, by the second enterprise official, that the encryption certificate be designated as recoverable;

querying the directory by the registration web server to verify that the second enterprise official is allowed to approve recovery of the encryption certificate of the user; and

signaling a key recovery authority by the registration web server to tag the encryption certificate of the user as recoverable.

11. The method according to claim 7, wherein the recovering the encryption certificate by the third enterprise official comprises:

accessing a registration web server by the third enterprise official;

sending a signature certificate of the third enterprise official to the registration web server by the third enterprise official to authenticate the third enterprise official to the registration web server;

requesting, by the third enterprise official, that the encryption certificate be recovered;

querying the directory by the registration web server to verify that the third enterprise official is allowed to recover the encryption certificate of the user; and

signaling a key recovery authority by the registration web server to send the encryption certificate of the user to the third enterprise official.

12. An article comprising a storage medium having instructions stored therein, the instructions when executed causing a processing device to perform:

receiving a signature certificate of a first enterprise official to authenticate the first enterprise official to the processing device;

receiving a request from the first enterprise official that an encryption certificate of a user be designated as recoverable;

querying a directory to verify that the first enterprise official is allowed to approve recovery of the encryption certificate of the user;

signaling a key recovery authority to tag the encryption certificate of the user as recoverable;

receiving a signature certificate of a second enterprise official to authenticate the second enterprise official to the processing device;

receiving a request from the second enterprise official that the encryption certificate be recovered;

querying the directory to verify that the second enterprise official is allowed to recover the encryption certificate of the user; and

signaling a key recovery authority to send the encryption certificate of the user to the second enterprise official.

13. The article according to claim 12, wherein the user is a current member of an enterprise that includes at least the processing device, the directory, the key recovery authority, the first enterprise official and the second enterprise official.

14. The article according to claim 12, wherein the user is a former member of an enterprise that includes at least the processing device, the directory, the key recovery authority, the first enterprise official and the second enterprise official.

15. The article according to claim 12, wherein the key recovery authority is an application on a server.

16. A system for third party recovery of encryption certificates in a Public Key Infrastructure (PKI) comprising:

a directory operably connected to a network, the directory containing information on at least one user, the directory further containing an enterprise official associated with each at least one user that is authorized to designate an encryption certificate of the at least one user as recoverable; and

at least one server operably connected to the network, at least one server receiving and processing requests for designating the encryption certificates of the at least one user as recoverable and requests for recovering the encryption certificates of the at least one user, at least one server sending the encryption certificate to an enterprise official after receiving authorization to send the encryption certificate to the enterprise official.

17. The system according to claim 16, wherein the directory comprises a database.

18. The system according to claim 16, further comprising a registration web page application resident on the first at least one server, the registration web page application receiving and processing the requests for designating the encryption certificate as recoverable and the requests for recovering the encryption certificate.

19. The system according to claim 16, further comprising a key recovery authority application resident on the second at least one server, the key recovery authority sending the encryption certificate to the enterprise official after receiving

the authorization from the first at least one server to send the encryption certificate to the enterprise official.

20. The system according to claim 16, wherein one at least one server performs the receiving and processing of requests for designating the encryption certificates of the at least one user as recoverable and requests for recovering the encryption certificates of the at least one user, and the sending the encryption certificate to the enterprise official after receiving authorization to send the encryption certificate to the enterprise official.